

【特許請求の範囲】

【請求項1】 ホームネットワーク内に接続された機器に対する操作端末からのアクセス管理を行なうホームネットワーク接続機器のアクセス管理装置であって、前記ホームネットワーク内に、ユーザ毎に機器単位のアクセス許可情報を持つアクセス管理テーブルを設けたことを特徴とするネットワーク接続機器のアクセス管理装置。

【請求項2】 前記請求項1に記載のネットワーク接続機器のアクセス管理装置において、前記アクセス管理テーブルは、前記操作端末の場所に依じたアクセス許可情報を持つことを特徴とするネットワーク接続機器のアクセス管理装置。

【請求項3】 前記請求項1又は2に記載のネットワーク接続機器のアクセス管理装置において、前記アクセス管理テーブルは、前記ホームネットワークにログインする際の第1のユーザ認証とは異なる第2のユーザ認証によりアクセスが許可され得るか否かを示すアクセス変更の許可情報を持つことを特徴とするネットワーク接続機器のアクセス管理装置。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】本発明は、ホームネットワーク内に接続された機器に対するアクセスを、ユーザや機器毎に管理することが可能なネットワーク接続機器のアクセス管理装置に関するものである。

【0002】

【従来の技術】ホームネットワーク内に接続された家庭内の情報機器や家電機器を、ホームネットワークに接続された他の機器により操作する場合、ユーザ認証によってホームネットワークにログインが許可されると、該ホームネットワークに接続されている機器を全て操作することが可能である。

【0003】図13はホームネットワークに接続された機器を操作する時の処理を示すフローチャートである。まず、ホームネットワークにログインし(1401)、コマンド入力待ちとなる(1402)。

【0004】操作端末から、ホームネットワークに接続された機器の操作コマンドを入力する(1403)と、当該機器にコマンドを発行する(1404)。このようにして、ホームネットワーク内に接続された機器を操作端末より操作することができる。

【0005】

【発明が解決しようとする課題】しかしながら、上述した従来の技術においては、ホームネットワークへのログインが許可されると、ホームネットワークに接続された全ての機器を操作することが可能であり、家族以外の人や子供などに操作させたくない機器がネットワーク内に存在する場合に、その機器に対するアクセスを制限することができない。

【0006】また、家族以外の人や子供がホームネットワーク内の機器を操作する場合、家族や大人がいる場合は操作できる機器を増やすというようにできないという問題があった。

【0007】さらに、例えば親の部屋にある機器を子供には操作させたくない場合や、その逆の場合など、アクセス制限を変更するのが望ましいが、ホームネットワーク内の機器を操作する時に、操作する場所によって、アクセス制限を変更することができないという問題があった。

【0008】そしてまた、ホームネットワーク内から操作する時と、ホームネットワーク外(外出先など)から操作する時とで操作できる機器を制限する、或いは、家からの距離によって操作する機器を制限する、というようにできないという問題があった。

【0009】本発明は、上記課題に鑑みてなされたものであり、機器毎、ユーザ毎、操作場所などによりアクセス管理を行ない、さらに、アクセスできる機器を変更することが可能なホームネットワーク接続機器のアクセス管理装置を提供するものである。

【0010】

【課題を解決するための手段】本願の第1の発明は、ホームネットワーク内に接続された機器に対する操作端末からのアクセス管理を行なうホームネットワーク接続機器のアクセス管理装置であって、前記ホームネットワーク内に、ユーザ毎に機器単位のアクセス許可情報を持つアクセス管理テーブルを設けたことを特徴とするものである。

【0011】これによって、例えば家族以外の人(ゲスト)や子供などに操作させたくない機器がホームネットワーク内に存在する時にも、ユーザ毎に設定された機器単位のアクセス許可情報に基づいて、操作させたくない機器に対するアクセスを制限することができる。

【0012】本願の第2の発明は、前記アクセス管理テーブルは、前記操作端末の場所に依じたアクセス許可情報を持つことを特徴とするものである。ここで、操作端末の場所とは、ホームネットワークからの距離、ホームネットワークが構築されている屋内の部屋、ホームネットワークの内外などによって規定される。

【0013】これによって、例えば操作する場所によって操作させたくない機器がホームネットワーク内に存在する場合にも、操作を行なう場所に依じたアクセス許可情報に基づいて、操作させたくない機器に対するアクセスを制限することができる。

【0014】また、操作する場所がホームネットワーク内か、ホームネットワーク外かによって操作させたくない機器がホームネットワーク内に存在する場合にも、操作させたくない機器に対するアクセスを制限することができる。

【0015】本願の第3の発明は、前記アクセス管理テ

10

20

30

40

50

3

ープルは、前記ホームネットワークにログインする際の第1のユーザ認証とは異なる第2のユーザ認証によりアクセスが許可され得るか否かを示すアクセス変更の許可情報を持つことを特徴とするものである。

【0016】これによって、例えば家族以外の人（ゲスト）や子供がホームネットワーク内の機器を操作する時に、第2のユーザ認証を行ない、認証されたユーザのアクセス許可情報に基づいて、家族や大人がいる場合は操作できる機器を増やすというようなことを実現することができる。

【0017】

【発明の実施の形態】以下、本発明の第1実施形態について、図1乃至図4とともに詳細に説明する。

【0018】図1は本実施形態におけるシステム構成例を示す説明図である。図1において、101はホームネットワーク111に接続される機器の管理や公衆ネットワーク112とホームネットワーク111との接続などをするホームゲートウェイ（以下、HGW）、102は各種情報を保管するデータベースである。

【0019】103、104、105、106はホームネットワーク111に接続された端末A、端末B、端末C、端末D、108、109、110は同じくホームネットワーク111に接続された無線端末A、無線端末B、無線端末C、107は無線端末A108、B109、C110を管理するアクセスポイント（AP）である。

【0020】尚、上記端末A103、B104、C105、D106および無線端末A108、B109、C110は、AV機器や、エアコン、湯沸し器等の家屋内にある電機製品や、パソコン等の情報機器、電話等の通信機器、それを操作するためのリモコン、PDA等である。

【0021】図2は本実施形態におけるアクセス管理テーブルを示す説明図である。このアクセス管理テーブル200は、図2に示すように、ホームネットワーク111に接続されるユーザ毎に機器単位のアクセス許可／不許可の情報を持つテーブルであり、ホームネットワーク111内のデータベース102、または、HGW101内などに保管されている。

【0022】前記アクセス管理テーブル200は、ホームネットワーク111に新たな機器を接続する場合に、ユーザ毎にその機器のアクセス許可／不許可情報が追加される。また、新しいユーザを登録する場合に、各機器に対して新しいユーザのアクセス許可／不許可情報が追加される。

【0023】図3はホームネットワーク111内に接続された機器を操作するための操作端末の一例を示すブロック図である。この操作端末300は、図3に示すように、ユーザに対して情報を提示する表示部301と、文字、画像、音声情報などを入力する入力部302と、ネ

4

ットワークと接続するネットワークインタフェース部303と、メモリ部304と、上記各部301～304をコントロールする処理部305とを有している。

【0024】図4は操作端末300からホームネットワーク111内の機器を操作する時の処理を示すフローチャートである。以下、図4を参照してユーザ毎に機器単位のアクセス管理を行なう方法を詳しく説明する。

【0025】まず、操作端末300の入力部302から、ユーザ名、パスワード等を入力し、ユーザのログインを行なう（401）。ここでは、操作端末300内のメモリ部304に記録されているユーザ情報により認証を行なうか、ネットワークインタフェース部303を介して、HGW101にユーザ名、パスワード等を送信して認証を行なう。

【0026】ユーザが認証されると、ホームネットワーク111内のデータベース102またはHGW101のアクセス管理テーブル200から、ログインしたユーザのアクセス制御テーブルを、ネットワークインタフェース部303を介して取得し（402）、メモリ部304に保存した後、操作コマンドの入力待ちになる（403）。

【0027】次に、入力部302から、ホームネットワーク111内の機器を操作する制御コマンドが入力される（404）と、メモリ部304内のアクセス制御テーブルとの照合を行なう（405）。

【0028】照合の結果、アクセス可能であれば、当該機器に対して制御コマンドをネットワークインタフェース部303を介して送信する（406）。アクセス不可能であれば、当該機器の制御が不可能であることをユーザに対して表示部301より通知し（407）、操作コマンドの入力待ちに戻る（403）。

【0029】以上のように、本実施形態においては、ホームネットワーク111内に、ユーザ毎に機器単位のアクセス許可／不許可情報を持つアクセス管理テーブル200を設けているので、ユーザ毎にホームネットワーク111に接続された機器単位のアクセス管理を行なうことができる。

【0030】次に、本発明の第2実施形態について、図5及び図6とともに説明するが、上記第1実施形態と同一部分には同一符号を付し、その説明は省略する。

【0031】本実施形態においては、ホームネットワーク111に接続されたアクセス管理装置を設けている。尚、このアクセス管理装置は、ホームネットワーク111を管理するHGW101に直接接続しても、HGW101に内蔵しても良い。

【0032】図5は本実施形態のアクセス管理装置を示すブロック図である。このアクセス管理装置600は、図5に示すように、ユーザ毎に機器単位のアクセス許可／不許可を示すテーブル情報や、ユーザの認証に必要な情報を保管するメモリ部601と、ネットワークと接続

するネットワークインタフェース部602と、上記各部601、602をコントロールする処理部603とを有している。

【0033】メモリ部601には、図2とともに上述した第1実施形態におけるアクセス管理テーブル200が保管される。上記第1実施形態と同様、ホームネットワーク111に新たな機器を接続する場合、ユーザ毎にその機器のアクセス許可／不許可情報をアクセス管理テーブル200に追加し、新しいユーザを登録する場合、各機器に対して新しいユーザのアクセス許可／不許可情報をアクセス管理テーブル200に追加する。

【0034】ホームネットワーク111に接続された機器は、図3とともに上述した第1実施形態における操作端末300を使用して操作される。図6は操作端末300からホームネットワーク111内の機器を操作する時の処理を示すフローチャートである。以下、図6を参照してユーザ毎に機器単位のアクセス管理を行なう方法を詳しく説明する。

【0035】まず、操作端末300の入力部302からユーザ名、パスワード等を入力し、ユーザのログインを行なう(701)。ここでは、操作端末300内のメモリ部304に記録されているユーザ情報により認証を行なうか、ネットワークインタフェース部303を介して、HGW101またはアクセス管理装置600内のメモリ部601の情報に基づき、ユーザ名、パスワード等を送信して認証を行なう。

【0036】ユーザが認証されると、操作コマンド入力待ちとなり(702)、入力部302から、ホームネットワーク111内の機器を操作する制御コマンドが入力される(703)と、ネットワークインタフェース部303を介して、アクセス管理装置600にユーザ情報と操作機器情報を送信し、制御の可否を確認する(704)。

【0037】この時、アクセス管理装置600では、メモリ部601に保存されているアクセス管理テーブル200の情報と受信したユーザ情報、操作機器情報とからアクセスの可否を判断し、判断結果を操作端末300へ送信する。

【0038】次に、アクセスが可能であれば、機器制御コマンドを制御対象の機器に対して送信し(705)、アクセス不可能であれば制御が不可能であることをユーザに対して表示部301より通知し(706)、操作コマンド入力待ち(702)に戻る。

【0039】以上のように、本実施形態においては、ホームネットワーク111内に、ユーザ毎に機器単位のアクセス許可／不許可情報を持つアクセス管理テーブル200を有するアクセス管理装置600を設けているので、ユーザ毎にホームネットワーク111に接続された機器毎のアクセス管理を行なうことができる。

【0040】尚、上述した第1実施形態においては、ロ

グイン時にHGWなどからアクセス管理テーブルの情報を取得するが、この場合ホームネットワークに接続されるどの機器に対してもアクセスする可能性があるので、すべての機器の情報を取得する必要があり、ログイン時に大量のデータが通信される。

【0041】これに対して、本実施形態においては、操作コマンド毎にアクセス管理装置に問い合わせる場合は、操作コマンドとユーザ情報とそれに対する許可／不許可の情報とが通信されるだけなので、通信データ量を低減させることが可能である。

【0042】また、上記第1実施形態では、アクセス管理テーブルとユーザ認証情報とが、別の機器に記録されている場合があるが、その場合、操作端末からコマンドを発行する時と認証の時とでそれぞれ別の機器に問い合わせなければならない。そこで、本実施形態においては、アクセス管理テーブルやユーザ認証情報などを一つの機器に記録しているので、操作端末から問い合わせる際に1つの機器で済む。

【0043】次に、本発明の第3実施形態について、図7及び図8とともに説明するが、上記第1実施形態と同一部分には同一符号を付し、その説明は省略する。

【0044】本実施形態においては、ホームネットワークに接続された機器を操作する機器の場所によってアクセス管理を行なうものであり、主にホームネットワーク外(屋外)からの操作に対するアクセス管理を行なうものである。

【0045】図7は本実施形態におけるアクセス管理テーブルを示す説明図である。このアクセス管理テーブル800は、図7に示すように、上記第1実施形態におけるアクセス管理テーブル200に、操作を行なう場所の情報を追加したものである。

【0046】ここで、操作を行なう場所の情報とは、例えば家と操作端末との距離であり、事前に各ユーザ、各機器毎に操作端末との距離に応じたアクセスの可または不可を決定し、アクセス管理テーブル800に登録しておく。

【0047】図8はホームネットワーク内に接続された機器を操作するための操作端末の一例を示すブロック図である。この操作端末900は、図8に示すように、ユーザに対して情報を提示する表示部901と、文字、画像、音声情報などを入力する入力部902と、ネットワークと接続するネットワークインタフェース部903と、メモリ部904とを有している。

【0048】さらに、GPSまたは公衆ネットワークの基地局等から送信される位置情報などに基づき、操作端末の位置情報を取得して保存する位置情報取得部905と、上記各部901～905をコントロールする処理部906とを有している。

【0049】上記位置情報取得部905は、一定の時間毎に位置情報を取得して更新するか、入力部902によ

10

20

30

40

50

7

り入力された命令によって位置情報を取得し更新する。

【0050】以下、操作端末900からホームネットワーク111内の機器を操作する時の処理（アクセス管理）について詳しく説明する。

【0051】まず、操作端末900の入力部902から、ユーザ名、パスワード等を入力し、ユーザのログインを行なう。ここでは、操作端末900内のメモリ部904に記録されているユーザ情報により認証を行なうか、ネットワークインターフェイス部909を介して、HGW101にユーザ名、パスワード等を送信して認証を行なう。

【0052】ユーザが認証されると、アクセス管理テーブル200を持つデータベース102またはHGW101などから、ログインしたユーザのアクセス制御テーブルをネットワークインターフェイス部903を介して取得し、メモリ部904に保存した後、操作コマンド入力待ちになる。

【0053】次に、入力部902から、ホームネットワーク111内の機器を操作する制御コマンドが入力されると、ログイン時のユーザ情報と入力されたコマンドとから得られる操作する機器の情報、位置情報取得部905の位置情報を、メモリ部904内のアクセス制御テーブルと照合する。

【0054】照合の結果、アクセス可能であれば、当該機器に対して制御コマンドをネットワークインターフェイス部903を介して送信し、アクセス不可能であれば、当該機器の制御が不可能であることをユーザに対して表示部901より通知し、操作コマンド入力待ちに戻る。

【0055】尚、ログイン時にHGW101などからユーザのアクセス制御テーブルを取得すると、通信するデータ量が増えるので、図6とともに上述した第2実施形態のような処理方法を行なうことにより、通信データ量を減らすことができる。

【0056】以上のように、本実施形態においては、ホームネットワーク111内に、各ユーザの場所（距離）毎に機器単位のアクセス許可／不許可情報を持つアクセス管理テーブル800を設けているので、ホームネットワーク111に接続された機器を操作する操作端末900の場所（距離）によって、アクセス管理を行なうことができる。

【0057】次に、本発明の第4実施形態について、図9とともに説明するが、上記第3実施形態と同一部分には同一符号を付し、その説明は省略する。

【0058】本実施形態においては、ホームネットワーク111に接続された機器を操作する機器の場所によってアクセス管理を行うものであり、主にホームネットワーク内（屋内）からの操作に対するアクセス管理を行うものである。

【0059】図9は本実施形態におけるアクセス管理テ

8

ーブルを示す説明図である。このアクセス管理テーブル1000は、図9に示すように、上記第1実施形態におけるアクセス管理テーブル200に、操作機器により操作を行なう場所の情報を追加したものである。

【0060】上記場所の情報とは、例えば操作する機器に対するアクセスを許す部屋のリストであり、事前に各ユーザ、各機器毎に操作端末のある部屋に応じたアクセスの可または不可を決定し、アクセス管理テーブル1000に登録しておく。

【0061】以下、操作端末900からホームネットワーク111内の機器を操作する時の処理（アクセス管理）について詳しく説明する。

【0062】まず、操作端末900の入力部902から、ユーザ名、パスワード等を入力し、ユーザのログインを行なう。ここでは、操作端末900内のメモリ部904に記録されているユーザ情報により認証を行なうか、ネットワークインターフェイス部909を介して、HGW101にユーザ名、パスワード等を送信して認証を行なう。

【0063】ユーザが認証されるとアクセス管理テーブル1000を持つデータベース102またはHGW101などから、ログインしたユーザのアクセス制御テーブルをネットワークインターフェイス部903を介して取得して、メモリ部904に保存した後、操作コマンド入力待ちになる。

【0064】次に、入力部902から、ホームネットワーク111内の機器を操作する制御コマンドが入力されると、位置情報取得部905の位置情報とメモリ部904内のアクセス制御テーブル1000とを照合する。

【0065】照合の結果、アクセス可能であれば、当該機器に対して制御コマンドをネットワークインターフェイス部903を介して送信し、アクセス不可能であれば、制御が不可能であることをユーザに対して表示部901より通知し、操作コマンド入力待ちに戻る。

【0066】尚、ログイン時にHGW101などからユーザのアクセス制御テーブルを取得すると、通信するデータ量が増えるので、図6とともに上述した第2実施形態のような処理方法を行なうことにより、通信データ量を減らすことができる。

【0067】以上のように、本実施形態においては、ホームネットワーク111内に、各ユーザの場所（部屋）毎に機器単位のアクセス許可／不許可情報を持つアクセス管理テーブル1000を設けているので、ホームネットワーク111に接続された機器を操作する操作端末900の場所（部屋）によって、アクセス管理を行なうことができる。

【0068】次に、本発明の第5実施形態について、図10とともに説明するが、上記第1実施形態と同一部分には同一符号を付し、その説明は省略する。

【0069】上述した第3実施形態および第4実施形態

9

をどちらも実施し、ホームネットワーク外（屋外）およびホームネットワーク内（屋内）の場所によって、アクセス管理を行なうことができるが、この場合、屋外の場合は距離毎に、屋内の場合は部屋毎に、アクセスの可否を決定し設定しておかなければならず、また、アクセス管理テーブルが大きくなる。

【0070】そこで、本実施形態においては、設定を簡略化するために、ホームネットワーク外からのアクセスと、ホームネットワーク内からのアクセスとの2通りのアクセスの可否を表すアクセス管理テーブルを備える。

【0071】図10は本実施形態におけるアクセス管理テーブルを示す説明図である。このアクセス管理テーブル1100は、図10に示すように、ホームネットワーク111外（屋外）、およびホームネットワーク111内（屋内）からのアクセス許可／不許可の情報を持つテーブルである。

【0072】以下、操作端末300からホームネットワーク111内の機器を操作する時の処理（アクセス管理）について詳しく説明する。

【0073】まず、操作端末300の入力部302から、ユーザ名、パスワード等を入力し、ユーザのログインを行なう。ここでは、ネットワークインターフェイス部303を介して、HGW101にユーザ名、パスワード等を送信して認証を行なう。

【0074】この時、HGW101はホームネットワーク111外からのアクセスかホームネットワーク内からのアクセスかを判断できるので、その判断結果を操作端末300に送信し、操作端末300はその情報をメモリ部304に記録する。

【0075】ユーザが認証されると、アクセス管理テーブル1100を持つデータベース102またはHGW101などから、ログインしたユーザのアクセス制御テーブルをネットワークインターフェイス部303を介して取得して、メモリ部304に保存、操作コマンド入力待ちになる。

【0076】次に、入力部302から、ホームネットワーク111内の機器を操作するコマンドが入力されると、ログイン時のユーザ情報と入力されたコマンドから得られる操作する機器の情報と、メモリ部304内の位置情報と、アクセス制御テーブルとを照合する。

【0077】照合の結果、アクセス可能であれば、当該機器に対して制御コマンドをネットワークインターフェイス部303を介して送信し、アクセス不可能であれば、制御が不可能であることをユーザに対して表示部301より通知して、操作コマンド入力待ちに戻る。

【0078】尚、ログイン時にHGW101などからユーザのアクセス制御テーブルを取得すると、通信するデータ量が増えるので、図6とともに上述した第2実施形態のような処理方法を行なうことにより、通信データ量を減らすことができる。

10

【0079】以上のように、本実施形態においては、ホームネットワーク111内に、各ユーザの場所（屋内外）毎に機器単位のアクセス許可／不許可情報を持つアクセス管理テーブル1100を設けているので、ホームネットワーク111に接続される機器を操作する操作端末300の場所（屋内外）によって、アクセス管理を行なうことができる。

【0080】次に、本発明の第6実施形態について、図11及び図12とともに説明するが、上記第1実施形態と同一部分には同一符号を付し、その説明は省略する。

【0081】本実施形態においては、ホームネットワーク111に接続された機器のアクセスの管理をユーザによって管理する時、第2のユーザ認識をすることによって、アクセスできるホームネットワーク内の機器を変更することができるものである。

【0082】図11は本実施形態におけるアクセス管理テーブルを示す説明図である。このアクセス管理テーブル1200は、図11に示すように、上記第1実施形態におけるアクセス管理テーブル200に、アクセス権限の変更の可否を表す情報を追加したものである。

【0083】前記アクセス管理テーブル1200は、ホームネットワーク111に新たな機器を接続する場合に、ユーザ毎にその機器のアクセス許可／不許可情報が追加される。また、新しいユーザを登録する場合に、各機器に対して新しいユーザのアクセス許可／不許可情報が追加される。

【0084】以下、操作端末300からホームネットワーク111内の機器を操作する時の処理（アクセス管理）について、特に第2のユーザ認識によりアクセスできるホームネットワーク111内の機器を変更する方法を、図12を用いて詳しく説明する。

【0085】まず、操作端末300の入力部302から、ユーザ名、パスワード等を入力し、ユーザのログインを行なう。ここでは、ネットワークインターフェイス部303を介して、HGW101にユーザ名、パスワード等を送信して第1のユーザ認証を行なう。

【0086】第1のユーザ認証がなされると、アクセス管理テーブル1200を持つデータベース102またはHGW101などから、ログインしたユーザのアクセス制御テーブルをネットワークインターフェイス部303を介して取得して、メモリ部304に保存した後、操作コマンド入力待ちになる。

【0087】次に、入力部302から、ホームネットワーク111内の機器を操作する制御コマンドを入力すると、メモリ部304内のアクセス制御テーブルとの照合を行ない、制御の可否を確認する。

【0088】ここで、ホームネットワーク111内の機器を操作できなかった時、アクセス管理テーブル1200を参照して、アクセス権限が変更可能であるか否かを判断する（1301）。

【0089】このとき、アクセス権限の変更が不可である場合は、制御が不可能であることをユーザに対して表示部301より通知し、操作コマンド入力待ちに戻る。

【0090】アクセス権限が変更可能である場合は、ユーザに対して第2のユーザ認証を行なうことにより操作できることを、表示部301より通知して(1302)、パスワードの入力要求を行なう(1303)。

【0091】ユーザは、第2のユーザ認証に必要なユーザ名、パスワード(ネットワークにログインする際の第1のユーザ認証に必要なパスワードとは異なるパスワード)等を入力する(1304)。

【0092】そして、操作端末300内のメモリ部304に記録されているユーザ情報により認証を行なうか、ネットワークインターフェイス部303を介して、HGW101にユーザ名、パスワード等を送信して第2のユーザ認証を行なう。

【0093】第2のユーザ認証がなされると、機器に対して制御コマンドをネットワークインターフェイス部303を介して送信し、第2のユーザ認証がなされなかった時は、制御が不可能であることをユーザに対して表示部301より通知し、操作コマンド入力待ちに戻る。

【0094】以上のように、本実施形態においては、ホームネットワーク111内に、各ユーザ毎に機器単位のアクセス権限の変更の可否を表す情報を持つアクセス管理テーブル1200を設けているので、第2のユーザ認証を行なうことによって、アクセスできるホームネットワーク111内の機器を変更することができる。

【0095】例えば、ある機器に対して、子供だけ有的时候には、アクセス(操作)させたくないが、親がそばにいたりときには、アクセス(操作)を許したいというような場合、第2のユーザ認証を行なうことにより、ホームネットワーク111にログインしたときの状態に比べて、アクセス(操作)できる機器を増やすことができる。

【0096】尚、本発明を実施するにあたっては、上述した各実施形態を組み合わせても良いことは明らかである。例えば、操作端末の場所に応じて、アクセス権限の変更可否を切り替えるなど、適宜実施することが可能である。

【0097】

【発明の効果】本願請求項1の発明によれば、例えば家族以外の人(ゲスト)や子供などに操作させたくない機器がホームネットワーク内に存在する時にも、ユーザ毎に設定された機器単位のアクセス許可情報に基づいて、操作させたくない機器に対するアクセスを制限することができる。

【0098】本願請求項2の発明によれば、例えば操作する場所によって操作させたくない機器がホームネットワーク内に存在する場合にも、操作を行なう場所に応じたアクセス許可情報に基づいて、操作させたくない機器

に対するアクセスを制限することができる。

【0099】また、操作する場所がホームネットワーク内か、ホームネットワーク外かによって操作させたくない機器がホームネットワーク内に存在する場合にも、操作させたくない機器に対するアクセスを制限することができる。

【0100】本願請求項3の発明によれば、例えば家族以外の人(ゲスト)や子供がホームネットワーク内の機器を操作する時に、第2のユーザ認証を行ない、認証されたユーザのアクセス許可情報に基づいて、家族や大人がいる場合は操作できる機器を増やすというようなことを実現することができる。

【図面の簡単な説明】

【図1】本発明の第1実施形態におけるシステム構成を示す説明図である。

【図2】本発明の第1実施形態におけるアクセス管理テーブルを示す説明図である。

【図3】本発明の第1実施形態における操作端末の概略構成例を示すブロック図である。

【図4】本発明の第1実施形態における操作端末からホームネットワーク内の機器を操作する時の処理を示すフローチャートである。

【図5】本発明の第2実施形態におけるアクセス管理装置を示す説明図である。

【図6】本発明の第2実施形態における操作端末からホームネットワーク内の機器を操作する時の処理を示すフローチャートである。

【図7】本発明の第3実施形態におけるアクセス管理テーブルを示す説明図である。

【図8】本発明の第3実施形態における操作端末の概略構成例を示すブロック図である。

【図9】本発明の第4実施形態におけるアクセス管理テーブルを示す説明図である。

【図10】本発明の第5実施形態におけるアクセス管理テーブルを示す説明図である。

【図11】本発明の第6実施形態におけるアクセス管理テーブルを示す説明図である。

【図12】本発明の第6実施形態における操作端末からホームネットワーク内の機器を操作する時の処理の要部を示すフローチャートである。

【図13】従来の操作端末からホームネットワーク内の機器を操作する時の処理を示すフローチャートである。

【符号の説明】

101 ホームゲートウェイ

102 データベース、

103~106 接続機器

107~110 無線端末

111 ホームネットワーク、

112 公衆ネットワーク

200、800、1000、1200 アクセス管理テ

13

ーブル

300、900 操作端末
 301、901 表示部
 302、902 入力部
 303、903 ネットワークインターフェイス部
 304、904 メモリ部

* 305、906 処理部

905 位置情報取得部

600 アクセス管理装置

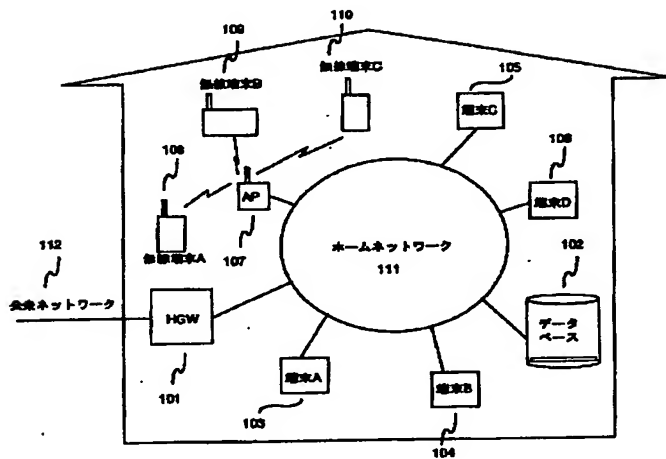
601 メモリ部

602 ネットワークインターフェイス部

* 603 処理部

14

【図1】



【図2】

200

| | 機器1 | 機器2 | 機器3 | 機器4 | 機器5 | 機器6 | 機器7 | 機器8 |
|------|-----|-----|-----|-----|-----|-----|-----|-----|
| 管理者 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| ユーザ1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| ユーザ2 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| ゲスト | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |

...

アクセス可 : 1
 アクセス不可 : 0

【図11】

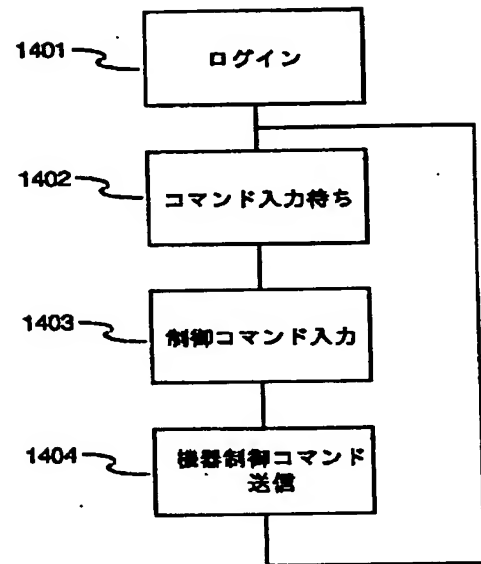
1200

| | 機器1 | 機器2 | 機器3 | 機器4 | 機器5 | 機器6 | 機器7 | 機器8 |
|------|-----|-----|-----|-----|-----|-----|-----|-----|
| 管理者 | 2 | 2 | 2 | 1 | 1 | 1 | 1 | 1 |
| ユーザ1 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| ユーザ2 | 0 | 0 | 2 | 2 | 1 | 1 | 1 | 1 |
| ゲスト | 0 | 0 | 0 | 0 | 2 | 2 | 1 | 1 |

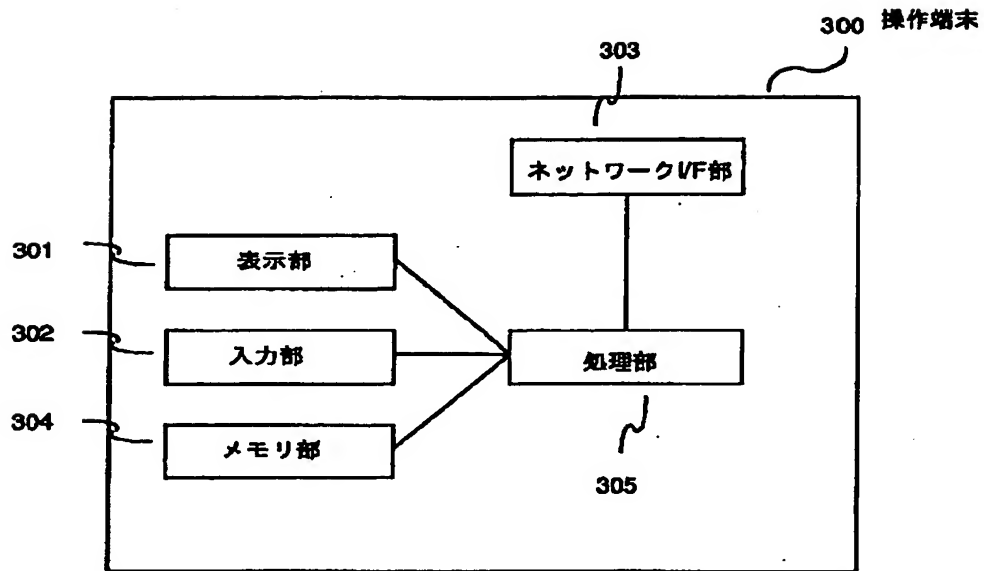
...

アクセス可 : 2
 アクセス変更可 : 1
 アクセス不可 : 0

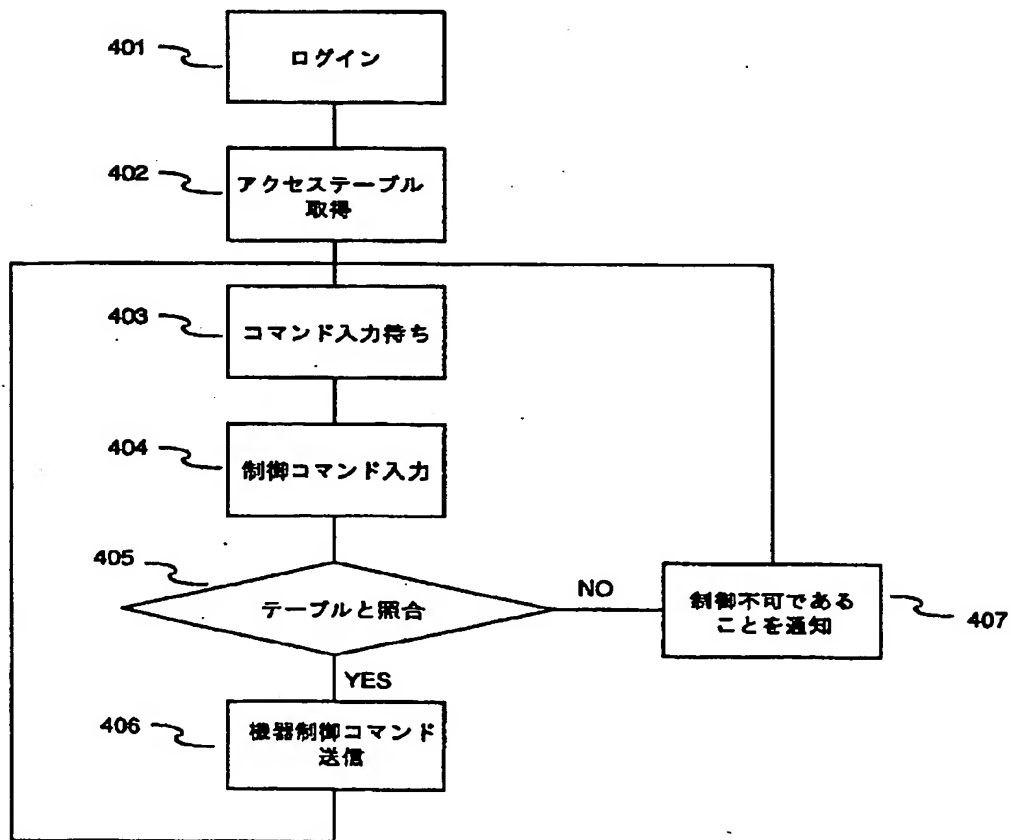
【図13】



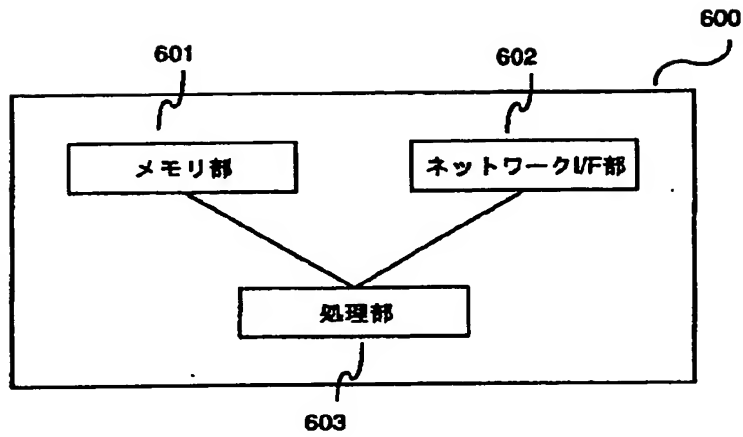
【図3】



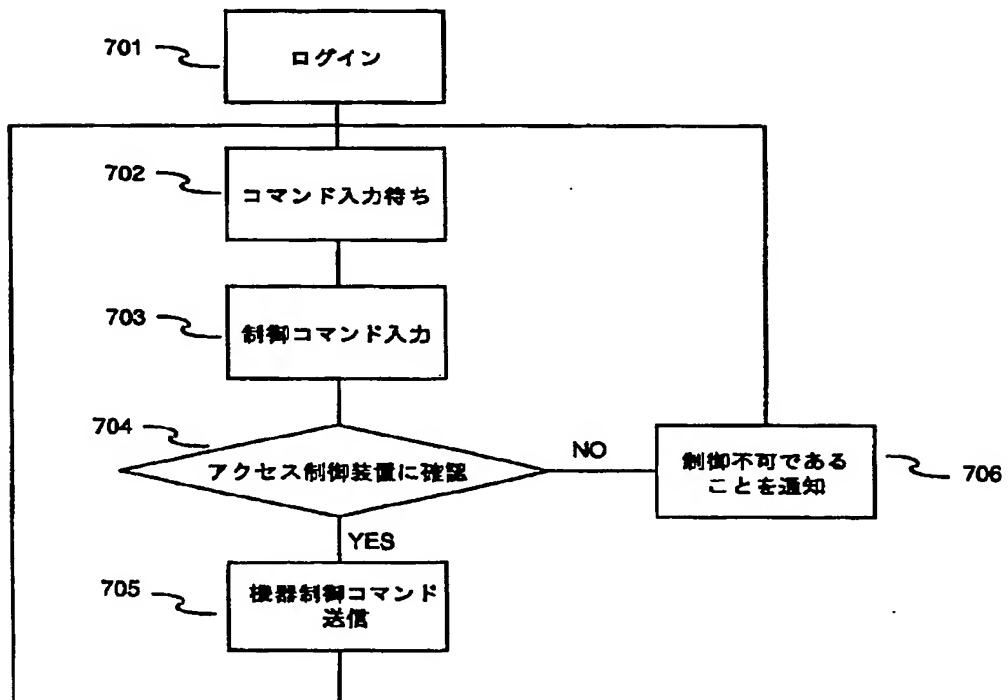
【図4】



【図5】



【図6】



【図7】

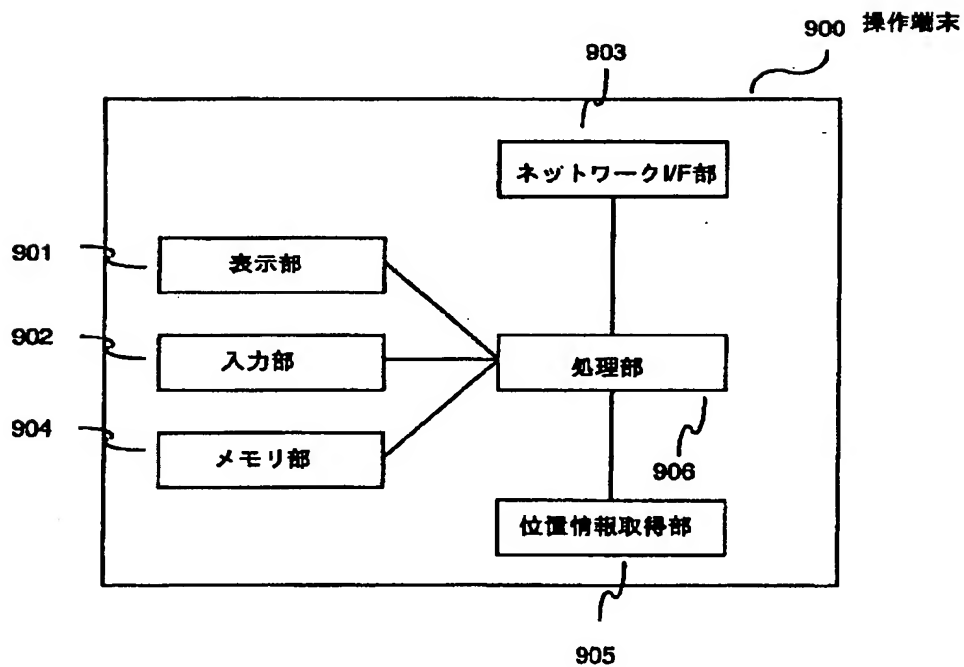
800

| | | 装置1 | 装置2 | 装置3 | 装置4 | 装置5 | 装置6 | 装置7 | 装置8 |
|------|--------|-----|-----|-----|-----|-----|-----|-----|-----|
| 管理用 | 100m以内 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | 1km以内 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| | それ以上 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| ユーザ1 | 100m以内 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| | 1km以内 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| | それ以上 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| ユーザ2 | 100m以内 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| | 1km以内 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| | それ以上 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| ゲスト | 100m以内 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 1km以内 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | それ以上 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

●
●
●

アクセス可 : 1
アクセス不可 : 0

【図8】



【図9】

1000
~

| | | 検器1 | 検器2 | 検器3 | 検器4 | 検器5 | 検器6 | 検器7 | 検器8 |
|------|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 管理者 | 部屋1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |
| | 部屋2 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |
| | 部屋3 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |
| ユーザ1 | 部屋1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |
| | 部屋2 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 |
| | 部屋3 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 |
| ユーザ2 | 部屋1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 |
| | 部屋2 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| | 部屋3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| ゲスト | 部屋1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| | 部屋2 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| | 部屋3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

●
●
●

アクセス可 : 1
アクセス不可 : 0

【図10】

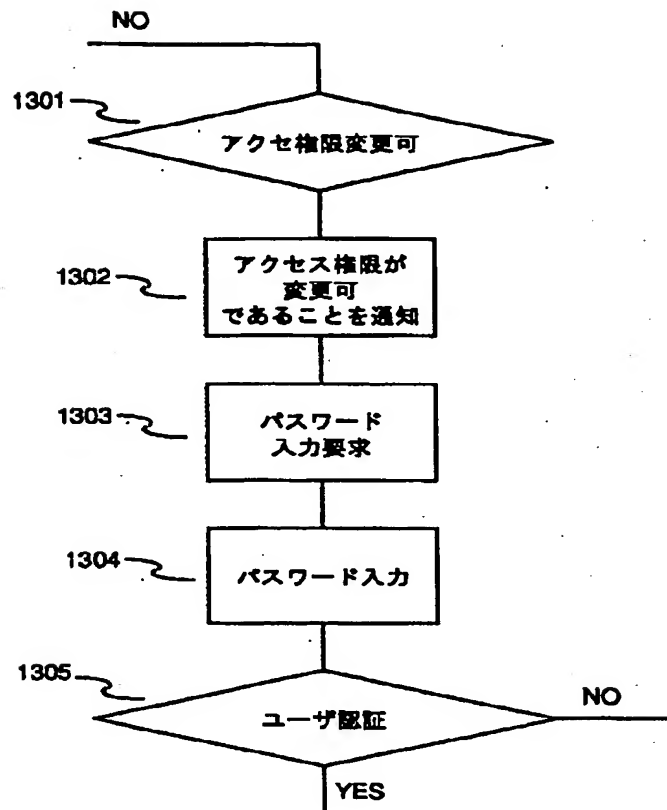
1100
~

| | | 検器1 | 検器2 | 検器3 | 検器4 | 検器5 | 検器6 | 検器7 | 検器8 |
|------|----|-----|-----|-----|-----|-----|-----|-----|-----|
| 管理者 | 屋内 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | 屋外 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| ユーザ1 | 屋内 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | 屋外 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| ユーザ2 | 屋内 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| | 屋外 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| ゲスト | 屋内 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| | 屋外 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

●
●
●

アクセス可 : 1
アクセス不可 : 0

【図12】



THIS PAGE BLANK (OPTION)